

Configurazione di Cisco Secure ACS per Windows v3.2 con autenticazione computer PEAP-MS-CHAPv2

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Nozioni di base](#)

[Convenzioni](#)

[Esempio di rete](#)

[Configurazione di Cisco Secure ACS per Windows v3.2](#)

[Ottenere un certificato per il server ACS](#)

[Configurazione di ACS per l'utilizzo di un certificato dall'archivio](#)

[Specificare Autorità di certificazione aggiuntive da considerare attendibili per ACS](#)

[Riavviare il servizio e configurare le impostazioni PEAP su ACS](#)

[Specificare e configurare il punto di accesso come client AAA](#)

[Configurare i database utente esterni](#)

[Riavvia il servizio](#)

[Configurazione di Cisco Access Point](#)

[Configurazione del client wireless](#)

[Configura registrazione automatica computer certificati Microsoft](#)

[Aggiungi al dominio](#)

[Installare manualmente il certificato radice nel client Windows](#)

[Configurazione della rete wireless](#)

[Verifica](#)

[Risoluzione dei problemi](#)

[Informazioni correlate](#)

[Introduzione](#)

In questo documento viene illustrato come configurare PEAP (Protected Extensible Authentication Protocol) con Cisco Secure ACS per Windows versione 3.2.

Per ulteriori informazioni su come configurare l'accesso wireless sicuro utilizzando i controller LAN wireless, il software Microsoft Windows 2003 e Cisco Secure Access Control Server (ACS) 4.0, fare riferimento a [PEAP in Unified Wireless Networks with ACS 4.0 and Windows 2003](#).

Prerequisiti

Requisiti

Non sono previsti prerequisiti specifici per questo documento.

Componenti usati

Le informazioni fornite in questo documento si basano sulle versioni software e hardware riportate di seguito.

- Cisco Secure ACS per Windows versione 3.2
- Servizi certificati Microsoft (installato come Autorità di certificazione radice dell'organizzazione [CA])**Nota:** per ulteriori informazioni, consultare la [Guida dettagliata all'impostazione di un'Autorità di certificazione](#) .
- Servizio DNS con Windows 2000 Server con Service Pack 3**Nota:** se si verificano problemi con il server CA, installare l'[hotfix 323172](#) . Il client Windows 2000 SP3 richiede l'[hotfix 313664](#) per abilitare l'autenticazione IEEE 802.1x.
- Cisco Aironet serie 1200 Wireless Access Point 12.01T
- IBM ThinkPad T30 con Windows XP Professional e Service Pack 1

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Nozioni di base

Sia PEAP che EAP-TLS creano e utilizzano un tunnel TLS/Secure Socket Layer (SSL). PEAP utilizza solo l'autenticazione sul lato server; solo il server dispone di un certificato e ne dimostra l'identità al client. EAP-TLS, tuttavia, utilizza l'autenticazione reciproca in cui sia il server ACS (Authentication, Authorization, and Accounting [AAA]) che i client dispongono di certificati e si scambiano le rispettive identità.

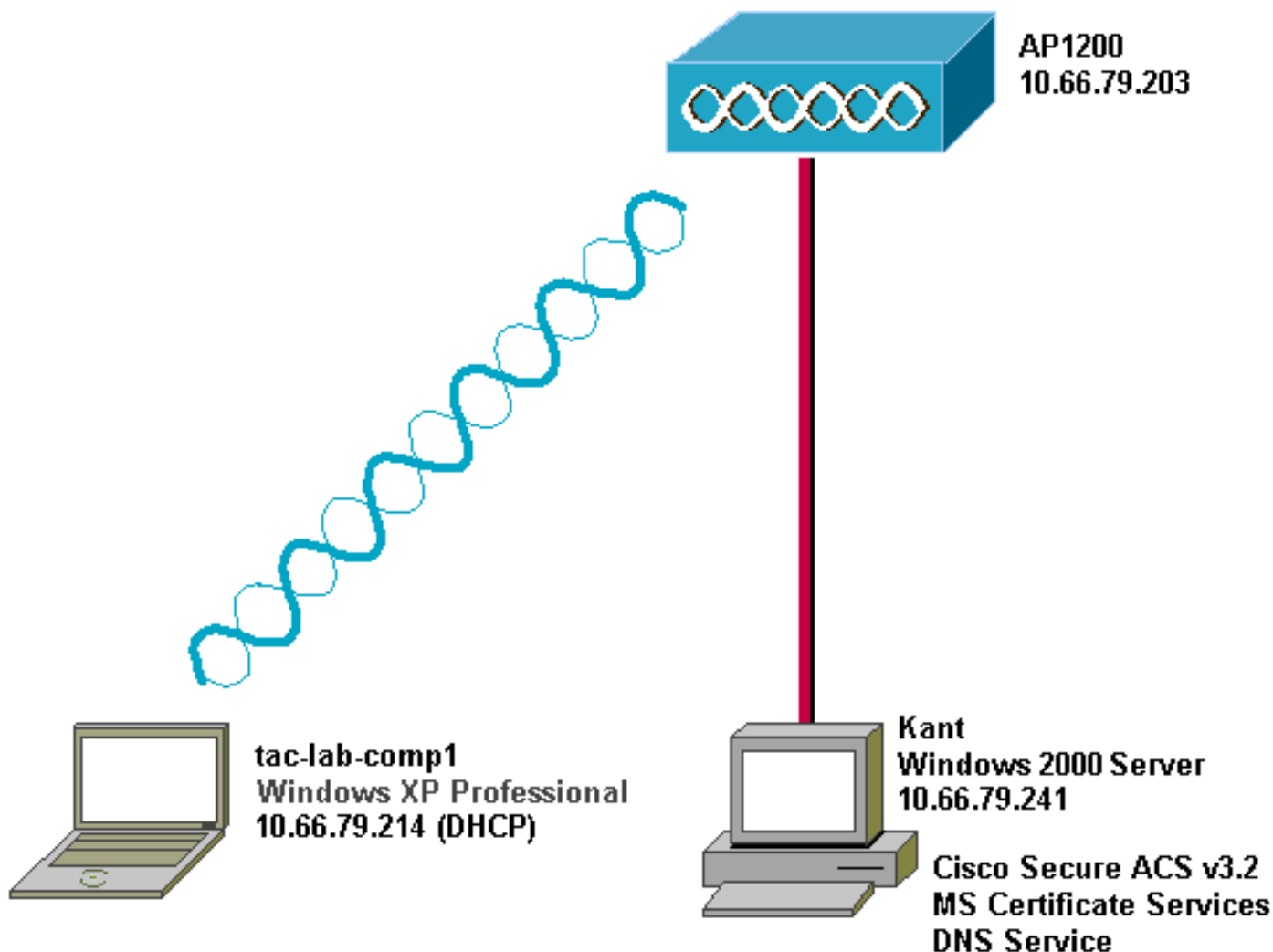
PEAP è utile perché i client non richiedono certificati. EAP-TLS è utile per l'autenticazione dei dispositivi headless, poiché i certificati non richiedono l'interazione dell'utente.

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento [Cisco sulle convenzioni nei suggerimenti tecnici](#).

Esempio di rete

Questo documento utilizza le impostazioni di rete mostrate nel diagramma sottostante.



Configurazione di Cisco Secure ACS per Windows v3.2

Per configurare ACS 3.2, attenersi alla seguente procedura.


1. [Ottenere un certificato per il server ACS.](#)
2. [Configurare ACS per l'utilizzo di un certificato di archiviazione.](#)
3. [Specificare le autorità di certificazione aggiuntive da considerare attendibili per ACS.](#)
4. [Riavviare il servizio e configurare le impostazioni PEAP su ACS.](#)
5. [Specificare e configurare il punto di accesso come client AAA.](#)
6. [Configurare i database utente esterni.](#)
7. [Riavviare il servizio.](#)

Ottenere un certificato per il server ACS

Per ottenere un certificato, eseguire la procedura seguente.

1. Sul server ACS, aprire un browser Web e individuare il server CA immettendo **http://CA-ip-address/certsrv** nella barra degli indirizzi. Accedere al dominio come

Enter Network Password [?] [X]

 Please type your user name and password.

Site: 10.66.79.241

User Name: Administrator

Password: *****

Domain: SEC-SYD

Save this password in your password list

OK Cancel

amministratore.

2. Selezionare **Richiedi certificato** e quindi fare clic su

Microsoft Certificate Services -- Our TAC CA [Home](#)

Welcome

You use this web site to request a certificate for your web browser, e-mail client, or other secure program. Once you acquire a certificate, you will be able to securely identify yourself to other people over the web, sign your e-mail messages, encrypt your e-mail messages, and more depending upon the type of certificate you request.

Select a task:

- Retrieve the CA certificate or certificate revocation list
- Request a certificate
- Check on a pending certificate

Next >

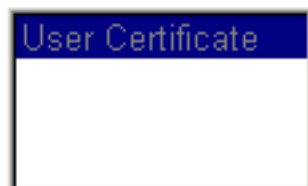
Avanti.

3. Selezionare **Richiesta avanzata**, quindi fare clic su

Choose Request Type

Please select the type of request you would like to make:

User certificate request:

A rectangular selection box with a blue header containing the text "User Certificate". The main body of the box is empty.

Advanced request

Next >

Avanti.

4. Selezionare **Invia una richiesta di certificato a questa CA utilizzando un modulo**, quindi fare clic su

Advanced Certificate Requests

You can request a certificate for yourself, another user, or a computer using one of the following methods. Note that the policy of the certification authority (CA) will determine the certificates that you can obtain.

- Submit a certificate request to this CA using a form.
- Submit a certificate request using a base64 encoded PKCS #10 file or a renewal request using a base64 encoded PKCS #7 file.
- Request a certificate for a smart card on behalf of another user using the Smart Card Enrollment Station.
You must have an enrollment agent certificate to submit a request for another user.

Next >

Avanti.

5. Configurare le opzioni del certificato. Selezionare **Server Web** come modello di certificato. Immettere il nome del server

Advanced Certificate Request

Certificate Template:

Web Server

Identifying Information For Offline Template:

Name: OurACS

E-Mail:

Company:

Department:

City:

State:

Country/Region: US

ACS.

Impo

stare la dimensione della chiave su **1024**. Selezionare le opzioni per **Contrassegna le chiavi come esportabili** e **Usa archivio locale del computer**. Configurare altre opzioni in base alle esigenze e quindi fare clic su

Key Options:

CSP:

Key Usage: Exchange Signature Both

Key Size: Min: 384 Max: 1024 (common key sizes: [512](#) [1024](#))

Create new key set
 Set the container name

Use existing key set

Enable strong private key protection

Mark keys as exportable
 Export keys to file

Use local machine store
You must be an administrator to generate a key in the local machine store.

Additional Options:

Hash Algorithm:
Only used to sign request.

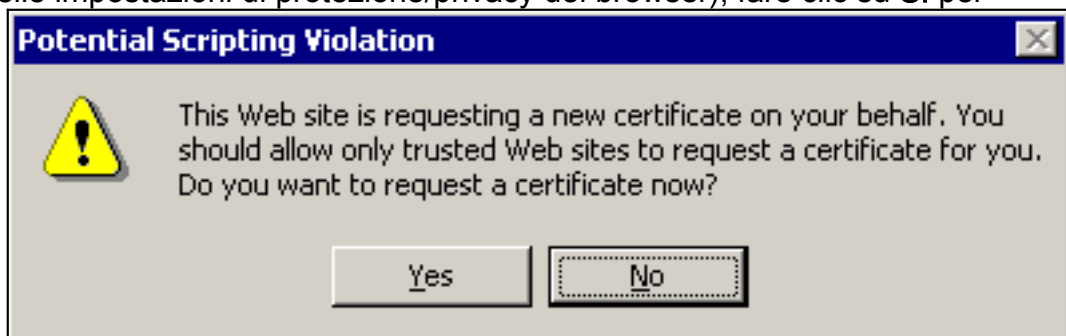
Save request to a PKCS #10 file

Attributes:

Invia.

Nota

: se viene visualizzata una finestra di avviso che fa riferimento a una violazione di script (a seconda delle impostazioni di protezione/privacy del browser), fare clic su **Sì** per




continuare.

6. Fare clic su **Installa il**

Microsoft Certificate Services -- Our TAC CA [Home](#)

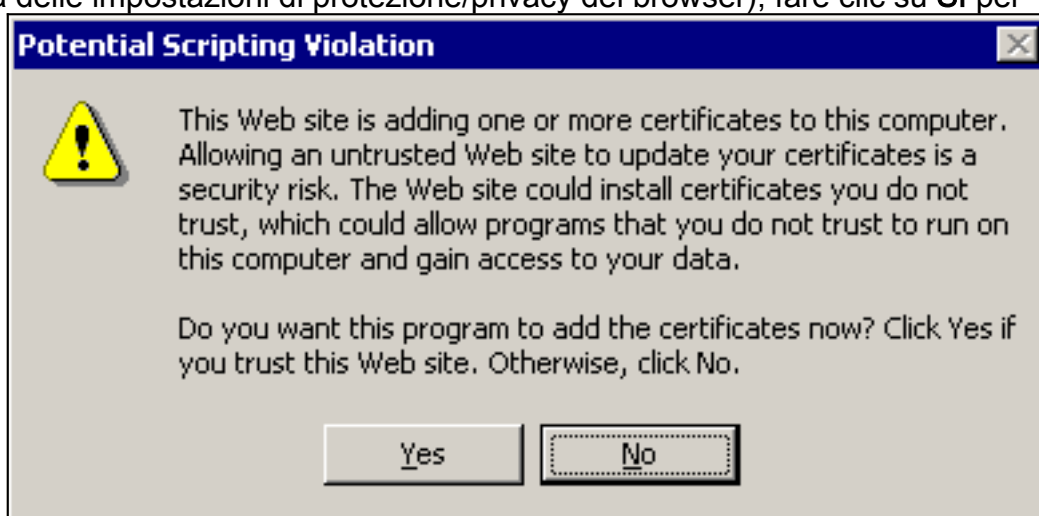
Certificate Issued

The certificate you requested was issued to you.

 [Install this certificate](#)

certificato.

Nota: se viene visualizzata una finestra di avviso che fa riferimento a una violazione di script (a seconda delle impostazioni di protezione/privacy del browser), fare clic su **Sì** per



continuare.

7. Se l'installazione è stata completata correttamente, verrà visualizzato un messaggio di

Microsoft Certificate Services -- Our TAC CA [Home](#)

Certificate Installed

Your new certificate has been successfully installed.

conferma.

[Configurazione di ACS per l'utilizzo di un certificato dall'archivio](#)

Per configurare ACS in modo da utilizzare il certificato in archiviazione, attenersi alla procedura seguente.

1. Aprire un browser Web e individuare il server ACS immettendo <http://ACS-ip-address:2002/> nella barra degli indirizzi. Fare clic su **Configurazione di sistema**, quindi su **Configurazione certificato ACS**.
2. Fare clic su **Installa certificato ACS**.
3. Selezionare **Usa certificato da archiviazione**. Nel campo CN certificato immettere il nome del

certificato assegnato al passaggio 5a della sezione [Ottenere un certificato per il server ACS](#). Fare clic su **Invia**. Questa voce deve corrispondere al nome digitato nel campo Nome durante la richiesta avanzata di certificati. È il nome della NC nel campo Oggetto del certificato del server; è possibile modificare il certificato del server per controllare il nome. Nell'esempio, il nome è "OurACS". *Non* immettere il nome CN dell'emittente.

The screenshot shows the Cisco System Configuration web interface. On the left is a navigation sidebar with icons and labels for: User Setup, Group Setup, Shared Profile Components, Network Configuration, System Configuration (highlighted), Interface Configuration, Administration Control, External User Databases, Reports and Activity, and Online Documentation. The main content area is titled "System Configuration" and "Edit". Below this is the "Install ACS Certificate" section. A sub-section titled "Install new certificate" contains two radio button options: "Read certificate from file" and "Use certificate from storage" (which is selected and circled in red). Below the selected option is a text input field for "Certificate CN" containing the text "OurACS", also circled in red. Further down are input fields for "Private key file" and "Private key password". At the bottom of the form area is a yellow "Back to Help" button with a question mark icon. At the very bottom are "Submit" and "Cancel" buttons.

4. Al termine della configurazione, verrà visualizzato un messaggio di conferma che indica che la configurazione del server ACS è stata modificata. **Nota:** al momento non è necessario riavviare

CISCO SYSTEMS

System Configuration

Edit

Install ACS Certificate

Installed Certificate Information ?

Issued to: OurACS
Issued by: Our TAC CA
Valid from: June 23 2003 at 02:19:56
Valid to: June 18 2005 at 00:52:30
Validity: OK

The current configuration has been changed. Restart ACS in "System Configuration:Service Control" to adopt the new settings for EAP-TLS or PEAP support only.

Install New Certificate Cancel

L'ACS.

[Specificare Autorità di certificazione aggiuntive da considerare attendibili per ACS](#)

L'ACS considererà automaticamente attendibile la CA che ha emesso il proprio certificato. Se i certificati client vengono emessi da CA aggiuntive, è necessario completare la procedura seguente.

1. Fare clic su **Configurazione di sistema**, quindi su **Configurazione certificato ACS**.
2. Fare clic su **Installazione Autorità di certificazione ACS** per aggiungere le CA all'elenco dei certificati attendibili. Nel campo relativo al file del certificato CA, immettere il percorso del certificato e fare clic su

CISCO SYSTEMS

System Configuration

Edit

ACS Certification Authority Setup

CA Operations 

Add new CA certificate to local certificate storage

CA certificate file

 Back to Help

User Setup

Group Setup

Shared Profile Components

Network Configuration

System Configuration

Interface Configuration

Administration Control

External User Databases

Reports and Activity

Online Documentation

Invia.

3. Fare clic su **Modifica elenco scopi consentiti ai certificati**. Selezionare tutte le CA che ACS deve considerare attendibili e deselezionare tutte le CA che ACS non deve considerare attendibili. Fare clic su

CISCO SYSTEMS

System Configuration

Edit

Edit Certificate Trust List

Edit the Certificate Trust List (CTL)

Display Name (Friendly Name)

- ABA.ECOM Root CA
(DST (ABA.ECOM) CA)
- Autoridad Certificadora de la Asociacion Na
(Autoridad Certificadora de la Asociacion N)
- Autoridad Certificadora del Colegio Nacional
- Baltimore EZ by DST
(DST (Baltimore EZ) CA)
- Belgacom E-Trust Primary CA
- C&W HKT SecureNet CA Class A
(CW HKT SecureNet CA Class A)
- C&W HKT SecureNet CA Class B
(CW HKT SecureNet CA Class B)

Invia.

[Riavviare il servizio e configurare le impostazioni PEAP su ACS](#)

Attenersi alla procedura seguente per riavviare il servizio e configurare le impostazioni PEAP.

1. Fare clic su **Configurazione di sistema** e quindi su **Controllo servizio**.
2. Fare clic su **Riavvia** per riavviare il servizio.
3. Per configurare le impostazioni PEAP, fare clic su **Configurazione di sistema**, quindi su **Configurazione autenticazione globale**.
4. Controllare le due impostazioni mostrate di seguito e lasciare tutte le altre impostazioni come predefinite. Se lo si desidera, è possibile specificare ulteriori impostazioni, ad esempio Abilita riconnessione rapida. Al termine, fare clic su **Invia**. **Consenti EAP-MSCHAPv2** **Consenti autenticazione MS-CHAP versione 2** **Nota:** per ulteriori informazioni su Fast Connect, fare riferimento a "Authentication Configuration Options" (Opzioni di configurazione autenticazione) in [System Configuration: Autenticazione e](#)

